News article

Feb 2022

Cyber Security Advisory - Escalating risk of cyber attack due to Ukraine/Russia situation

We're advising you that this situation presents a heightened risk of a cyber-attack to UK organisations and we want to help you minimise the risk to your business. The expectation is that any action taken by Russia will be conducted within cyber space.

Neil Robertson
VCISO Lead

Email neil.robertson@waterstons.com

The UK National Cyber Security Centre (NCSC) have recently published advice for organisations here, which we've summarised below. Please note this is not an exhaustive list of cyber security recommendations but rather a prioritised list of immediate actions that can be taken to reduce your risk exposure at the current time.

1. Assess your Security Patching

- Heighten your security patching response times, particular for those systems that are internet facing
- Conduct a network vulnerability scan of your network to validate where there are risks that a malicious attacker could exploit

2. Perform a Light Security Assessment / Health Check

- Ensure that MFA functionality is enabled on all internet facing systems
- Validate that your security alerts on key systems are appropriately configured and actively monitored (e.g. AV / Firewalls / EDR tools etc)
- Ensure a "offline" or "air-gapped" backup of your data is in place and has been recently tested to ensure it can be used to restore key data and services

3. Equip your staff to identify and report potential cyber threats

- Make your staff aware of the importance of identifying and reporting suspicious activity which could be the early indicators of a cyber attack
- Ensure staff are aware of their responsibilities e.g. using unique and secure passwords, reporting phishing emails and protecting
- company assets

4. Be prepared to execute your cyber response plan

- Put your Incident Management Team on warning
- Ensure that key responsibilities, partnerships and action plans are in place to coordinate the response to a potential cyber incident
- Conduct a “desktop rehearsal” of your cyber response plans to validate their effectiveness.

We will continue to monitor the threat landscape and provide critical updates to ensure you can take the action needed to safeguard your organisation.

If you’re concerned about your organisation’s security posture, our cyber team are here. Whether it’s a first step on your cyber journey to help get the basics in place, develop and evolve cyber secure working strategies across your organisation, provide support and training for your colleagues or provide 24 hour monitoring of your networks and infrastructure we can help.